Synergy.net™ Product Software Security

Arthrex Imaging and Resection

Introduction

Using the Secure Product Development Framework (SPDF) approach, Arthrex strives to design and develop secure products. The SPDF process contains the suggested steps and best practices for addressing security and privacy throughout the software product life cycle, including during the design, development, production, distribution, deployment, and maintenance of an electronic medical device or software produced by Arthrex.

Building Security Into Arthrex Products

The effort to build security into Arthrex products is driven by industry best practices along with premarket and postmarket regulatory guidance. During the SPDF process, the Product Development Security Engineering group works with the Development, Product Management, Integrations, and Support teams to promote a comprehensive, security-conscious approach and culture to foster the delivery of secure products.

Secure Product Development Framework

As part of every product's SPDF the following tasks are required where appropriate:

- **Security training:** Role-based training specific to product security and privacy
- **Security planning:** Integrating security in the design process
- **Product security requirements scorecard:** Security standards for the development team to follow
- **Threat modeling and risk analysis:** Identifying security flaws and risks in the product design
- **Open-source software and third-party software validation:** Identifying and fixing vulnerabilities in software components
- **Static code analysis:** Using automated tools to detect defects and security flaws in code
- **Vulnerability scanning:** Using automated tools to detect security vulnerabilities in running systems
- **Penetration testing:** Attempting to circumvent security controls and uncover vulnerabilities in running systems
- **Security review:** Examining the results of the Security Development Lifecycle (SDL) activities
- **Production monitoring:** Surveilling software and systems for new threats or issues using automated tools and customer feedback

Conclusion

Arthrex is dedicated to building secure products by establishing oversight procedures that identify and mitigate potential product security risks during development and creating programs and practices that drive software security initiatives and awareness across the company.

System Introduction

The Synergy.net system is a data synchronization and EHR integration platform. It allows each Synergy camera console on the facility network to synchronize surgeon, procedure, and preference settings to create a unified and consistent user experience. EHR integration provides additional efficiency improvements by automating patient worklists as well as exporting to a PACS or Vendor Neutral Archive (VNA).

Because it is a software application solely intended to transfer, store, convert formats, and display medical device data, the Synergy.net system is classified as a Medical Device Data System (MDDS).

The Synergy.net system must be installed and hosted on a customer-provided server, typically a virtual server running a Microsoft Windows Server operating system. The customer is responsible for managing the operating system and anti-virus software.

System Introduction (cont.)

The Synergy.net™ system has the following features:

- Surgeon procedure and preference synchronization among multiple Synergy camera consoles
- Centralized database for surgeon preferences
- Centralized synchronization of surgical stills and videos
- EHR interoperability via HL7
- DICOM video export
- Automated SurgeonVault® system upload for premium surgeon accounts
- Network printing
- Text messages of case status

Arthrex Governance Policies and Practices

- Information Security Manager
- Corporate Information Security Policy (ISO27001)
- Privacy and Compliance Manager
- Corporate Privacy and Compliance Policy (HIPAA-HITECH)
- Incident Response Policy
- Disaster Recovery and Business Continuity Policy
- High Assurance Agile Software Development Lifecycle

Figure 1. System Diagram

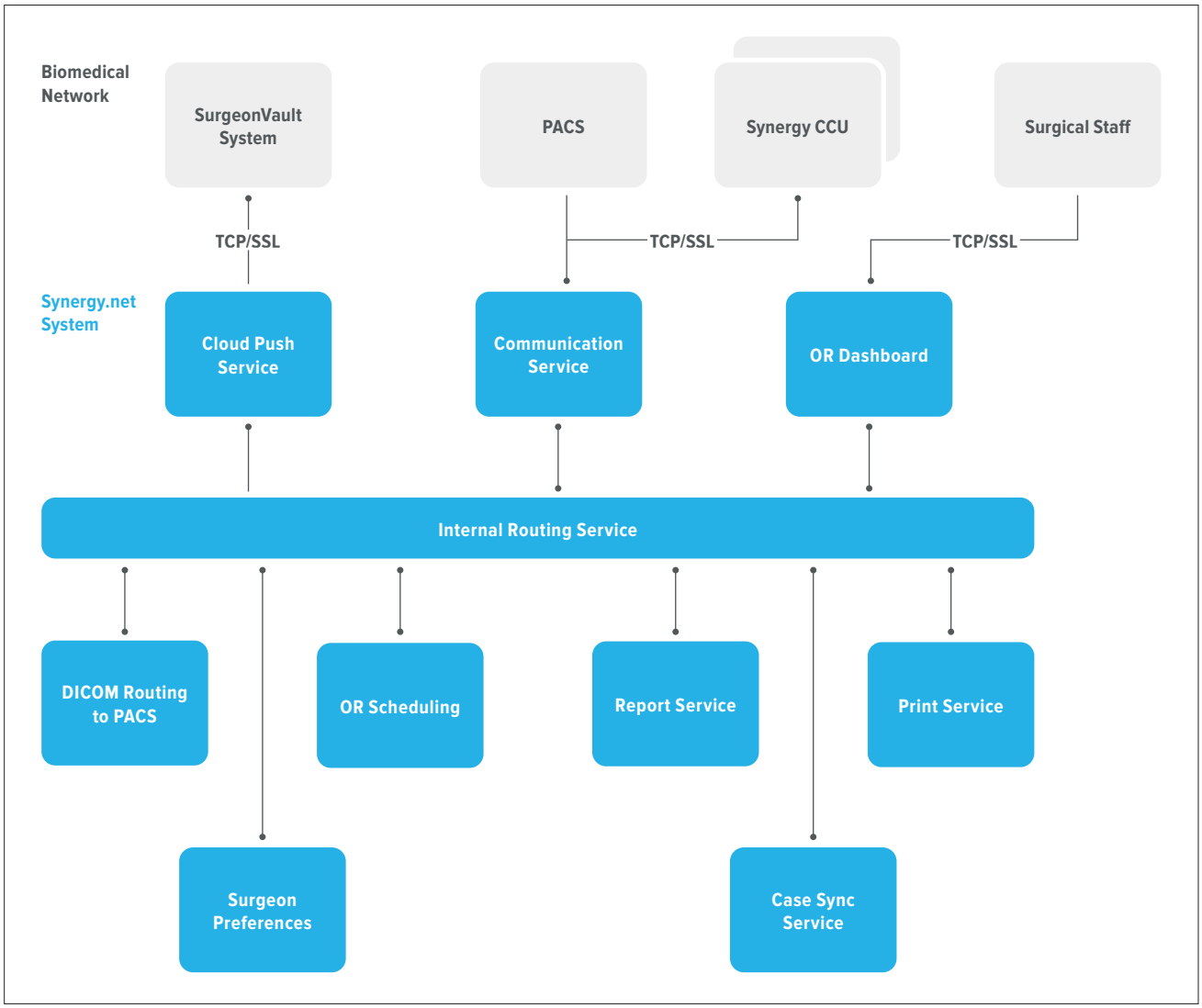

Table 1. System Controls Information

System Access and Use Overview	The Synergy.net™ system is a MDDS software application installed on customer provided server.
Operating System	Not applicable. The Synergy.net system is a software application installed on customer-deployed Microsoft Windows Server operating system.
System Data Classification	Private Health Information
Data Storage	Data is stored locally with export options to the SurgeonVault® system, PACS, or VNA.
Data Security	TLS 1.2 is used for data in transit. The hosting server can be deployed with full disk encryption.
Data Export	Data may be exported to the SurgeonVault system, PACS server, or VNA.
Data Deletion	Software removal and corresponding data is the responsibility of local facilities per their policies and procedures.
Retention	This software is not intended to be used as a permanent archive (eg, PACS) for data retention.
Network Security	Secure connections using TLS encryption or SSH are required for encryption of data in transit.
Certificates	• Arthrex uses commercially available encryption certificates. • The Synergy.net system operates using two private public key infrastructures (PKIs): one global PKI with the Synergy Root CA as the trust anchor and the other a per-site PKI with the local Synergy.net server as the trust anchor. The two PKIs are independent (ie, the per-site root is not signed by the global CA) because the local server is inherently untrusted outside of the site and should not be able to issue certificates that are trusted by other sites.
Authentication	• Local authentication using password complexity rules (eg, uppercase, lowercase, number, symbol) are enforced. • Authentication using local facility's LDAP services may be configured and the facility's LDAP password policies inherited.
Authorization	Role-based access control (RBAC) is used.
Audit Logging	Audit logs are recorded as event types to the Windows Event Manager. The following events are logged: • Successful login • Unsuccessful login • Logout • View case • View case list • Export case • Print case • Delete case • Create case
Accountability	Arthrex is responsible for providing patches and upgrades for the Synergy.net system. The customer is responsible for patching and upgrading of the Microsoft Windows operating system.
Software Patching/ Upgrade	• Arthrex is the sole developer of the Synergy.net system and maintains software patches and upgrades for the system. • Updates are cryptographically signed and will be installed only if the signature is correct.
Support	Support for the Synergy.net system can be obtained through telephone or email communication.